HP SURE START
INFOBLATT

HP WOLF SECURITY

HP Sure Start[1] ist eine fortschrittliche hardwaregestützte Lösung, die umfassende Sicherheit für Firmware und Firmware-Einstellungen bietet. HP Sure Start begann als weltweit erstes selbstheilendes BIOS und geht jetzt darüber hinaus, um kritische Firmware zu schützen, die von Antivirenlösungen nicht geschützt werden kann. HP Sure Start bietet hardwaregestützten, selbstheilenden Schutz der bootkritischen Firmware vor Malware, Root-Kits oder Verletzungen, um die Geschäftskontinuität auch bei destruktiven Angriffen auf die Firmware aufrechtzuerhalten.

FIRMWARE-ANGRIFFE STELLEN EINE AKTUELLE BEDROHUNG DAR

MosaicRegressor, LoJax und andere Formen von BIOS-Angriffen haben sich zu neuen Bedrohungskategorien für PCs entwickelt. Diese Angriffe sind schwierig zu erkennen, persistent und schwer zu entfernen. Sie sind leistungsstark und erlangen die volle Kontrolle über einen PC mit der höchsten Berechtigungsstufe.

Wenn Malware das BIOS oder kritische Firmware angreift, kann der Angreifer wertvolle Daten stehlen, Ransomware einschleusen oder Ihren PC funktionsunfähig machen.

Hardwaregestützter Schutz und Ausfallsicherheit für das BIOS und andere kritische Firmware sind beim Hochfahren und während des Betriebs wichtiger denn je.

HARDWAREGESTÜTZTER SCHUTZ

Seit 2014 wird HP Sure Start durch ein einzigartiges Hardwareelement unterstützt: den HP Endpoint Security Controller.

HP Sure Start nutzt den HP Endpoint Security Controller für einen starken, hardwarebasierten Schutz des Codes, der Daten und der Geheimnisse, die im BIOS und in der kritischen Firmware gespeichert sind.

DAS ERSTE BIOS DER BRANCHE MIT AUTOMATISCHER FEHLERBEHEBUNG

Angefangen mit dem weltweit ersten hardwareunterstützten, selbstheilenden BIOS-Schutz und nach mehreren Generationen von Verbesserungen bietet HP Sure Start heute die umfassendste PC-Firmware-Schutz- und Ausfallsicherheitslösung auf dem Markt an.

Im Falle eines Malware-Angriffs auf das BIOS oder die kritische Firmware erkennt HP Sure Start den Eingriff automatisch, benachrichtigt den Benutzer, protokolliert das Ereignis für die IT-Abteilung und stellt die letzte einwandfreie Version des BIOS oder der Firmware wieder her.

HP Sure Start erkennt alle nicht autorisierten Änderungen am BIOS oder an kritischer Firmware, anstatt nach bekannter Malware zu suchen. Das bedeutet, dass HP Sure Start Sie vor Angriffen schützen kann, die es so noch nie gegeben hat.

VERWALTBARKEIT

HP Sure Start sorgt für automatischen Schutz, der zentral von Ihrem IT-Team verwaltet werden kann. Mit den folgenden Verwaltungslösungen können Sie die HP Sure Start Einstellungen remote einstellen und Manipulationsalarme überwachen.

- Microsoft® System Center Configuration Manager über das HP Manageability Integration Kit[2] (HP MIK)-Plug-in.
- Die HP Client Management Script Library ist ein leistungsstarkes Tool, das eine einfache Integration in jede auch noch so moderne Verwaltungskonsole ermöglicht.

EINZIGARTIGER FIRMWARE-SCHUTZ

HP Sure Start verfügt über eine einzigartige und stabile Auswahl an Schutzfunktionen.

- Schutz sowohl vor der Ausführung der Firmware als auch während der Laufzeit
- Zum Schutz von CODE und DATEN
- Intel Manageability Engine-Firmware/AMD Secure Processor/CPU-Mikrocode
- Kryptografisch geschützte Speicherung von Einstellungen und Geheimnissen
- Dedizierter/isolierter Speicher für Richtlinien und Wiederherstellungsfirmware
- Auch aktiv, wenn der PC ausgeschaltet ist. Arbeitet unabhängig vom Hauptprozessor
- Schützt vor Angriffen durch direkten Speicherzugriff bei geschlossenen und offenen Gehäusen

UNTERSTÜTZUNG DES PRODUKTPORTFOLIOS

HP Sure Start ist ab Werk in vielen kommerziellen Produkten des HP Portfolios enthalten.

- ZBook und Z-Workstations
- Pro- und Elite-Notebooks und Desktop-PCs (Intel vPro- und nicht-vPro- sowie AMD-Prozessoren)
- Auswahl von RPOS und Thin Clients

ZERTIFIKATE UND NORMEN

ZERTIFIZIERTE HARDWARE

Der HP Endpoint Security Controller, der in den HP Sure Start Plattformen verwendet wird, wurde von einem akkreditierten, unabhängigen Testlabor auf die von HP gemäß den öffentlich verfügbaren Kriterien, Methoden und Prozessen geforderten Betriebsbedingungen überprüft.

NIST-RICHTLINIEN

Die HP Sure Start Plattformen gehen deutlich über die NIST-Richtlinien für die Ausfallsicherheit von Boot-Firmware für Host-Prozessoren hinaus und schützen auch eine Reihe anderer bootkritischer Firmware.

(Sonderveröffentlichung 800-193).

Weitere Informationen finden Sie hier:
HP Sure Start Whitepaper.

HÄUFIG GESTELLTE FRAGEN

F: Was muss ich tun, um von den Vorteilen von HP Sure Start zu profitieren?
A: HP Sure Start ist standardmäßig für alle Anwendungsplattformen aktiviert, die ab Werk von HP ausgeliefert werden. Es besteht keine Notwendigkeit, die Funktion zu aktivieren oder anderweitig „bereitzustellen". Wenn Ihr Gerät mit HP Sure Start ausgeliefert wird, sind Sie ab dem ersten Start geschützt.

F: Mein Unternehmen verwendet ein benutzerdefiniertes Software-Image. Wird HP Sure Start durch ein erneutes Imaging des Geräts gelöscht?
A: HP Sure Start ist hardwaregestützt und im BIOS untergebracht. Durch ein erneute Imaging des Computers wird es nicht gelöscht oder der Überwachungs- und Selbstheilungsschutz des BIOS und der kritischen Firmware deaktiviert.

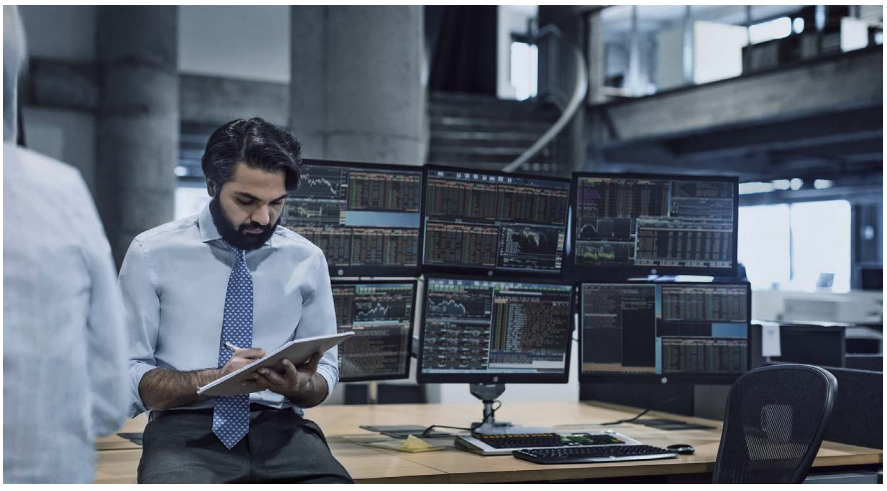
Bestimmte betriebssystemabhängige Funktionen von HP Sure Start (z. B. Remote-Laufzeitüberwachung oder BS-interne Benachrichtigungen im Windows® Event Viewer) können je nach verwendetem Betriebssystem geändert oder deaktiviert werden.

F: Ich habe ein wachsendes Unternehmen, aber keine IT-Abteilung. Kann ich HP Sure Start trotzdem nutzen?
A: Ja. Da HP Sure Start standardmäßig aktiviert ist, sind Sie automatisch geschützt. Es besteht kein IT-Handlungsbedarf.

F: Was sind DMA-Angriffe (Direct Memory Access)?
A: Ein DMA-Angriff ist ein Angriff, bei dem ein Angreifer periphere Hardware nutzt, um alle vorhandenen Zugriffssteuerungen für den Betriebssystemspeicher zu umgehen und so den Hauptspeicher des Betriebssystems direkt auszulesen oder zu überschreiben. Systeme mit HP Sure Start nutzen eine Virtualisierungshardware, um böswillige DMAs zu blockieren.

F: Gegen welche Art von Angriffen schützt HP Sure Start?
A: HP Sure Start schützt vor nicht autorisierten Änderungen am BIOS und an kritischem Firmware-Code oder an den BIOS-Einstellungen, sowohl für den Systemstart- als auch für den Laufzeitcode. Diese Funktionen schützen Sie vor einer Vielzahl unterschiedlicher Angriffe, einschließlich neuer Firmware-Angriffe, die in Zukunft auftreten könnten.

F: Wenn Malware das BIOS angreifen kann, warum kann sie dann nicht die BIOS-Kopie von HP Sure Start beschädigen?
A: HP setzt eine einzigartige Technologie ein, die vom HP Endpoint Security Controller unterstützt wird, um die saubere HP Sure Start Kopie des BIOS und der kritischen Firmware von der Kopie des BIOS und der kritischen Firmware zu isolieren, die vom Gerät verwendet werden. Dies geschieht hardwaregeschützt und ist für Hacker unzugänglich.



[1] HP Sure Start der 6. Generation ist auf ausgewählten HP PCs verfügbar und erfordert Windows 10.
[2] Das HP Manageability Integration Kit kann unter http://www.hp.com/go/clientmanagement heruntergeladen werden.

Mehr dazu unter hp.com/go/computer security.

HP WOLF SECURITY

4AA7-2562DEE, Mai 2021